UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/749,142	12/27/2000	Thomas Wille	DE000002	4761

24737 7590 07/16/2004

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/749,142	WILLE ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/27/2000*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 have been examined.

Specification

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

3. The abstract of the disclosure is objected to because: remove the word "Figure" at the bottom of the abstract. Correction is required.

Claim Objections

4. Claim 14 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim. See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claim 5 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The claim recites "in the sense of current consumption, a cryptographic operation is split up into two mutually complementary operations". However, the disclosure fails to teach how to split up, in the sense of current consumption, a cryptographic operation is into two mutually complementary operations. Thus, the disclosure fails to enable one skilled in the art to make and use the claimed invention.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1, 6 and 10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claims 1 and 10, a broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10 USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" and then narrow language. The Board stated that this can render a claim indefinite by raising a

question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949). In the present instance, claims 1 and 10 recite the broad recitation "a data processing device" (1st line), and the claim also recites "particularly a chip card or smart card" (1st line) which is the narrower statement of the range/limitation.

b. Regarding claims 1 and 10, the word "particular" (1st line) renders the claims indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

c. Regarding claim 6, the two operations are mutually complementary (see claim 5). As such, it is interpreted as that one operation is complementary of the other but not that one operation is complementary and the other is not complementary. Thus, it is not clear what the feature "which processor performs the operation complementary or not complementary" means.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1, 4-5, 7 and 9-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Patarin et al. (6,658,569).

a. Regarding claim 1, which is representative of claim 10, Patarin discloses a method of operating a data-processing device, with an integrated circuit comprising a central processing unit and one or more co-processors, in which the integrated circuit performs cryptographic operations, characterized in that in performing a cryptographic operation in the integrated circuit, at least two processors perform a cryptographic operation simultaneously and in parallel (Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40).

b. Regarding claims 4 and 11, Patarin further discloses that a cryptographic operation is split up into at least two sub-operations and in that at least two processors perform the sub-operations in parallel and simultaneously (Fig. 2, step A; col. 12, lines 6-12 and 31-40).

c. Regarding claim 5, mutually complementary operations in the sense of current consumption are interpreted as operations that when executed minimize or eliminate information leaks from cryptographic systems that result from power consumption fluctuations. Patarin discloses that the cryptographic operation is split up into two operations (col. 5, lines 13-17) that when executed eliminate information leaks from cryptographic systems that result from power consumption fluctuations (col. 3, lines 11-

14). Thus, the two operations disclosed by Patarin meets the limitation of mutually complementary operations in the sense of current consumption.

d. Regarding claims 7 and 12, Patarin further discloses that a cryptographic operation is split up into at least two sub-operations, and the sub-operations are performed simultaneously and in parallel by the processors while subsequently corresponding sub-results are combined to an overall result of the overall cryptographic operation (Fig. 2; col. 12, lines 6-12 and 31-40).

e. Regarding claim 9, Patarin further discloses that the sub-operations are parts of an encryption in accordance with DES (col. 5, lines 10-14).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 2, 4-5 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin as applied to claim 1 and 12 above, and further in view of Jahnich et al. (6,725,374).

a. Regarding claim 2 and 13, Patarin does not teach the use of dummy operations in cryptography. Jahnich discloses using dummy programs, whose execution does not influence an encryption result (col. 6, lines 32-48); the dummy programs meet the

limitation of dummy operations. It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Patarin to use dummy operations, as taught by Jahnich. The execution of the dummy operations causes additional advantageous current fluctuations to be observed in a DPA analysis and thus contributes to the confusion of an attacker.

b. Regarding claims 4, Patarin further discloses that a cryptographic operation is split up into at least two sub-operations and in that at least two processors perform the sub-operations in parallel and simultaneously (Fig. 2, step A; col. 12, lines 6-12 and 31-40).

c. Regarding claim 5, mutually complementary operations in the sense of current consumption are interpreted as operations that when executed minimize or eliminate information leaks from cryptographic systems that result from power consumption fluctuations. Patarin discloses that the cryptographic operation is split up into two operations (col. 5, lines 13-17) that when executed eliminate information leaks from cryptographic systems that result from power consumption fluctuations (col. 3, lines 11-14). Thus, the two operations disclosed by Patarin meets the limitation of mutually complementary operations in the sense of current consumption.

13. Claims 3-6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Jahnich as applied to claims 2, 7 and 13 above, and further in view of Tan (6,490,353).

a. Regarding claims 3 and 14, Patarin and Jahnich do not disclose that the selection of a processor to perform a cryptographic operation is randomly controlled. Tan discloses that that the selection of a processor to perform a certain cryptographic operation is randomly controlled (col. 3, lines 60-64; col. 6, lines 6-12). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Jahnich such that the selection of a processor to perform a cryptographic operation is randomly controlled, as taught by Tan, so that security could further be enhanced.

b. Regarding claims 4, Patarin further discloses that a cryptographic operation is split up into at least two sub-operations and in that at least two processors perform the sub-operations in parallel and simultaneously (Fig. 2, step A; col. 12, lines 6-12 and 31-40).

c. Regarding claim 5, mutually complementary operations in the sense of current consumption are interpreted as operations that when executed minimize or eliminate information leaks from cryptographic systems that result from power consumption fluctuations. Patarin discloses that the cryptographic operation is split up into two operations (col. 5, lines 13-17) that when executed eliminate information leaks from cryptographic systems that result from power consumption fluctuations (col. 3, lines 11-14). Thus, the two operations disclosed by Patarin meets the limitation of mutually complementary operations in the sense of current consumption.

d. Regarding claim 6, the feature "which processor performs the operation complementary or not complementary" is interpreted as "which processor performs

which of the two mutually complementary operations". Patarin and Jahnich do not disclose that the selection of which processor to perform which of the two mutually complementary operations. Tan discloses that that the selection of a processor to perform a certain cryptographic operation is randomly controlled (col. 3, lines 60-64; col. 6, lines 3-12). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Jahnich such that the selection of a processor to perform a cryptographic operation is randomly controlled, as taught by Tan, so that security could further be enhanced.

14. Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin as applied to claim 7 above, and further in view of Tan.

a. Regarding claim 8, Patarin does not disclose that the split-up of the cryptographic operation is randomly controlled. Tan discloses that data to be encrypted is segmented into blocks and that the size of each data block and length of the corresponding encryption key for each block are randomly selected (col. 3, lines 8-42); the selection of the block size and the key length meet the limitation of splitting up a cryptographic operation. It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin such that the split-up of the cryptographic operation is randomly controlled, as taught by Tan, to increase the degree of difficulty in attacking the encryption system.

b. Regarding claim 9, Patarin further discloses that the sub-operations are parts of an encryption in accordance with DES (col. 5, lines 10-14).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Feyt et al. (WO 99/49416) discloses a method for hiding protected operations performed in microprocessor cards.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Minh Dinh
Examiner
Art Unit 2132

MD
7/9/2004

JUSTIN T. DARROW
PRIMARY EXAMINER